UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/456,692	12/09/1999	STEVEN G. FRY	M-7916US	6777

33031 7590 10/19/2007
CAMPBELL STEPHENSON LLP
11401 CENTURY OAKS TERRACE
BLDG. H, SUITE 250
AUSTIN, TX 78758

EXAMINER	
COLIN, CARL G	
ART UNIT	PAPER NUMBER
2136	

NOTIFICATION DATE	DELIVERY MODE
10/19/2007	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

lclark@cspatents.com
bbrock@cspatents.com

Office Action Summary	**Application No.** 09/456,692	**Applicant(s)** FRY ET AL.	
	Examiner Carl Colin	**Art Unit** 2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *02 August 2007*.

2a)☒ This action is **FINAL**. 2b)□ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *107-147 and 165-181* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *107-147 and 165-181* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) ☒ Interview Summary (PTO-413)
Paper No(s)/Mail Date. *20071010* .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

DETAILED ACTION

Response to Arguments

1. In response to communications filed on 9/28/2007, the following claims 107-147 and 165-181 are presented for examination.

1.1. Applicant's arguments, filed on 9/28/2007 have been fully considered but they are not persuasive as amended. Applicant argues that Killian discloses a network address and the network address is not a token in any respect. Examiner respectfully disagrees because according to Applicant's specification, page 12, lines 5-8, the specification recites "Although passwords need not be employed, some method of determining which in-bound connections are to be coupled to other in-bound connections should be supported by the relay program. Other such methods may include for example the use of network addresses, the use of verification strings, and the like." Therefore, in light of the specification, Examiner's interpretation of network address as token is very reasonable. Applicant has amended the dependent claims to remove the word network address as a security token. However, the claims as amended can still read on a token as a verification string because a string can be broadly and reasonably interpreted as a sequence of character. In response to Applicant's remarks that Kilian does not disclose associating afirst security token with a first connection. Examiner respectfully disagrees (see column 13, lines 1-10; column 14, lines 60-64 and column 5, lines 15-33) disclosing associating a socket for each connection (process of communications between end systems) and maintaining a connection table for associating a security token (such as network address) with each connection. Upon further consideration, the claims as amended have not overcome the prior art. Therefore, Examiner maintains rejection of claims in view of the same prior art.

Claim Objections

2. Claim 131 and the intervening claims are objected to because of the following informalities: claim 131 recites "means for creating means for associating". The claim limitation will be interpreted as "means for creating comprises means for associating". Appropriate correction is required.

Claim Rejections - 35 USC § 101

3. 35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims 165, 174, and the intervening claims are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. The claims recite a computer program comprising instructions executable by a processor. The computer program recited in the preamble without a computer-readable medium needed to realize the computer program's functionality is non-statutory functional descriptive material. See MPEP § 2106.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 107-115, 131-139, and 165-173 are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent 6,064,671 to **Killian** in view of US Patent 6,643,701 to **Aziz et al.**

As per claim 107, **Killian** discloses a method comprising: providing a plurality of sockets in a socket table or array, wherein each socket normally represents a connection (i.e. has an associated connection) and each socket has an associated network port and network IP address (see column 14, lines 52-64 and column 15, lines 60-67 and column 5, lines 15-22) that meets the recitation of *providing a plurality of sockets, wherein each socket has an associated connection and an associated security token* (network address);

Killian discloses the network address is provided by the associated connection (see column 6, lines 31-36 and lines 41-50) that meets the recitation of *the associated security token is provided by the associated connection*;

Killian also discloses receiving an outgoing message having a network address (see column 7, line 65 through column 8, line 2) and the message is associated with a connection (see column 29, lines 41-42), the message is also associated with a socket (see column 28, lines 26-27), that meets the recitation of *receiving a first connection and a first security token*;

Killian further discloses creating a socket and each socket has an associated connection (see column 14, lines 60-64 and column 5, lines 15-33) that meets the recitation of *creating a socket associated with the first connection,*

wherein the creating comprises associating the first security token (network address) *with the first connection* (see column 13, lines 1-10; column 14, lines 60-64 and column 5, lines 15-40);

Killian further discloses comparing the network address with the associated network addresses for a match in the socket table (see column 16, lines 6-12) that meets the recitation *of comparing the first security token with the associated security tokens*;

in response to said comparing if none of the associated security tokens match the first security token (see column 16, lines 17-20)*, including the socket in the plurality of sockets* (see column 16, lines 25-28).

Although **Killian's** disclosure referring to message is interpreted as a connection, it is obvious to one of ordinary skill in the art that the message is directed to a connection as explained above because it is associated with socket and as disclosed also in column 5, lines 52-60, the message is transmitted over a connection. It would have been obvious to one of ordinary skill in the art at the time the invention was made to use the disclosure of Killian of routing message to route connection between physical networks for internetworking (see column 1, lines

45-65). **Aziz et al** in an analogous art teaches end to end security link by creating a first end-to-end security link between the first computer and a third computer and creating a second end-to-end security link between the second computer and the third computer to establish the secure connection (see column 3, lines 35-56 and column 7, line 56 through column 8, line 5). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine Killian and Aziz et al to create two separate connections at each end system to provide an application-specific authentication and link them to establish a secure connection between two end systems when messages are exchanged between computers.

As per claim 108, the references as combined above disclose the limitation of wherein the security token is one of a password and a verification string (see **Killian** column 14, lines 52-64 and column 5, lines 15-40).

As per claim 109, Killian discloses in response to said comparing when a match occurs coupling an end point of the first connection to a network interface or to a machine which has a connection to the network at a remote location (see column 19, lines 4-7 and column 28, lines 38-46). **Aziz et al** discloses linking an end point of a first connection to an end point of a second connection in response to authentication (see column 7, line 49 through column 8, line 5), the authentication may include an authentication token such as password (see column 2, lines 10-15). Claim 109 is rejected on the same rationale as the rejection of claim 107.

As per claim 110, the references as combined above disclose the limitation of in response to said comparing, if none of the associated security tokens match the first security token, upon a determination that the first connection is not to be associated with a socket, disconnecting the first connection (see **Killian** column 22, lines 43-47).

As per claim 111, the references as combined above disclose wherein the coupling the first connection to the connection associated with the socket comprises: relaying a data stream between the first connection and the connection associated with the socket (see **Killian,** column 28, lines 38-46) and (see **Aziz et al,** column 7, line 49 through column 8, line 5).

As per claim 112, the references as combined above disclose wherein the coupling the first connection to the connection associated with the socket comprises: creating a single connection comprising the first connection and the connection associated with the socket (see **Killian,** column 19, lines 4-7 and column 28, lines 38-46) and (see **Aziz et al,** column 7, line 65 through column 8, line 1).

As per claim 113, the references as combined above disclose decoupling the first connection and the connection associated with the socket (see **Killian,** column 22, lines 30-42).

As per claim 114, the references as combined above disclose the decoupling occurs upon one of failure and disconnect of one of the first connection and the connection associated with the socket (see **Killian,** column 22, lines 42-47).

As per claim 115, the references as combined above disclose wherein the first connection is transmitted through a first firewall program (see **Killian,** column 24, lines 48-59).

As per claim 131, **Killian** discloses an apparatus comprising: figures 8 and 13 for instance show computer systems for performing the claimed method of claim 1 comprising means for providing a plurality of sockets in a socket table or array, wherein each socket normally represents a connection (i.e. has an associated connection) and each socket has an associated network port and network IP address (see column 14, lines 52-64 and column 15, lines 60-67 and column 5, lines 15-22) that meets the recitation of *means for providing a plurality of sockets, wherein each socket has an associated connection and an associated security token* (network address);

Killian discloses the network address is provided by the associated connection (see column 6, lines 31-36 and lines 41-50) that meets the recitation of *the associated security token is provided by the associated connection*;

Killian also discloses end system and router (computer system) including means for receiving an outgoing message having a network address (see column 7, line 65 through column 8, line 2 and figs. 3-5) and the message is associated with a connection (see column 29, lines 41-42), the message is also associated with a socket (see column 28, lines 26-27), that meets the recitation of *means for receiving a first connection and a first security token*;

Killian further discloses computer system with means for creating a socket and each socket has an associated connection (see column 14, lines 60-64 and column 5, lines 15-33 and fig. 3 and fig. 13) that meets the recitation of *means for creating a socket associated with the first connection,*

wherein means for creating comprises means for associating the first security token (network address) *with the first connection* (see column 13, lines 1-10; column 14, lines 60-64 and column 5, lines 15-40);

Killian further discloses means for comparing the network address with the associated network addresses for a match in the socket table (see column 16, lines 6-12 and fig. 3) that meets the recitation *of means for comparing the first security token with the associated security tokens*;

in response to said comparing if none of the associated security tokens match the first security token (see column 16, lines 17-20), *means for including the socket in the plurality of sockets* (see column 16, lines 25-28).

Although **Killian's** disclosure referring to message is interpreted as a connection, it is obvious to one of ordinary skill in the art that the message is directed to a connection as explained above because it is associated with socket and as disclosed also in column 5, lines 52-60, the message is transmitted over a connection. It would have been obvious to one of ordinary skill in the art at the time the invention was made to use the disclosure of Killian of routing message to route connection between physical networks for internetworking (see column 1, lines 45-65). **Aziz et al** in an analogous art teaches end to end security link by creating a first end-to-end security link between the first computer and a third computer and creating a second end-to-end security link between the second computer and the third computer to establish the secure connection (see column 3, lines 35-56 and column 7, line 56 through column 8, line 5).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine Killian and Aziz et al to create two separate connections at each end system to provide an application-specific authentication and link them to establish a secure connection between two end systems when messages are exchanged between computers.

As per claim 132, the references as combined above disclose the limitation of wherein the security token is one of a password and a verification string (see **Killian** column 14, lines 52-64 and column 5, lines 15-40).

As per claim 133, Killian discloses in response to said comparing when a match occurs coupling an end point of the first connection to a network interface or to a machine which has a connection to the network at a remote location (see column 19, lines 4-7 and column 28, lines 38-46). **Aziz et al** discloses a relay (220 and 440, figures 2 and 4) having means for linking an end point of a first connection to an end point of a second connection in response to authentication (see column 7, line 49 through column 8, line 5), the authentication may include an authentication token such as password (see column 2, lines 10-15). Claim 133 is rejected on the same rationale as the rejection of claim 131.

As per claim 134, the references as combined above disclose the limitation of in response to said comparing, if none of the associated security tokens match the first security token, upon a determination that the first connection is not to be associated with a socket, means for disconnecting the first connection (see **Killian** column 22, lines 43-47).

As per claim 135, the references as combined above disclose wherein the coupling the first connection to the connection associated with the socket comprises: means for relaying a data stream between the first connection and the connection associated with the socket (see **Killian,** column 28, lines 38-46) and (see **Aziz et al,** column 7, line 49 through column 8, line 5).

As per claim 136, the references as combined above disclose wherein the coupling the first connection to the connection associated with the socket comprises: computer system such as the one shown in fig. 13 with means for creating a single connection comprising the first connection and the connection associated with the socket (see **Killian,** column 19, lines 4-7 and column 28, lines 38-46) and (see **Aziz et al,** column 7, line 65 through column 8, line 1).

As per claim 137, the references as combined above disclose means for decoupling the first connection and the connection associated with the socket (see **Killian,** column 22, lines 30-42 and fig. 13, 90B).

As per claim 138, the references as combined above disclose the decoupling occurs upon one of failure and disconnect of one of the first connection and the connection associated with the socket (see **Killian,** column 22, lines 42-47).

As per claim 139, the references as combined above disclose wherein the first connection is transmitted through a first firewall program (see **Killian,** column 24, lines 48-59).

As per claim 165, claim 165 discloses the same limitations as claim 107 except for incorporating the claimed method into a computer program. **Killian** discloses the computer systems include applications for performing the invention (see column 14, lines 44-64). Therefore, claim 165 is rejected on the same rationale as the rejection of claim 107. The associating step of claim 165 contrarily to claim 107 merely recites instructions configured to cause the processor to *associate the first security token* (network address) *with the first connection* (see column 13, lines 1-10; column 14, lines 60-64 and column 5, lines 15-40);

As per claim 166, the references as combined above disclose the limitation of wherein the security token is one of a password and a verification string (see **Killian** column 14, lines 52-64 and column 5, lines 15-40).

Claims 167-173 are similar to the rejected claims 109-115 respectively except for incorporating the claimed methods into a computer program. Therefore, 109-115 are rejected on the same rationale as the rejection of claims 167-173.

5. **Claims 116-119** are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent 6,064,671 to **Killian** in view of US Patent 6,643,701 to **Aziz et al** as applied to claims 107-115 and further in view of US Patent 6,104,716 to **Crichton et al**.

As per claims 116-119, **Killian** discloses a protocol daemon that can create network connections (column 21, lines 24-30 and lines 45-52) and discloses the first program providing a security token (see column 22, lines 8-20) but does not explicitly disclose the protocol daemon couples the first connection to the second connection. **Aziz et al** discloses a relay program for relaying first connection with second connection (see abstract and column 9, lines 30-39), either the client, the server, or the relay may be a protocol daemon (see column 6, lines 4-6), but does not explicitly disclose a second connection connecting the protocol daemon to the first program. **Crichton et al** in an analogous art teaches using a client proxy for communicating with a client and with a middle proxy and coupling the connections to provide end-to-end connections through firewalls (column 2, lines 26-52). **Crichton et al** also discloses the client and the proxy can reside on the same machine (column 6, lines 15-24). **Crichton et al** also discloses that the functionality of end proxies that meets the recitation of protocol daemon can be increased to allow for other protocols and services, for example one end proxy could provide both client and server end proxy functionality (column 5, lines 41-45). **Crichton et al** discloses one end proxy could provide both client and server end proxy functionality (column 5, lines 41-45). This means if the first program represents an application server an in-bound connection is created "a server end-proxy can connect to an inside X-Windows system server and a middle proxy" (column 5, lines 32-35). Applicant's specification discloses the same (on page 9, lines 9-15) program 135 (first program) requires an in-bound connection (e.g. where program 135 is an application server) … such functionality is provided by a daemon running on computer 105. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the proxy or protocol daemon disclosed in **Killian** and **Aziz et al** as combined above to provide a protocol daemon program that does the creating of the first connection as well as the second connection and coupling the first and second connections thus increasing the functionality of end proxy to allow for other protocols and services as suggested by **Crichton et al** (see column 5, lines 32-45). One skilled in the art would have been lead to make such a modification and recognizes the advantage of using an end proxy that could provide both client and server end proxy functionality as this increase of functionality would allow for more protocols and services as suggested by **Crichton et al** (see column 5, lines 41-45).

6. **Claims 120-124, 128-130, 140-144, and 174-178** are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent 6,643,701 to **Aziz et al** in view of US Patent 6,104,716 to **Crichton et al**.

As per claim 120, Aziz et al discloses a method comprising: receiving from a client or first computer (first program) a first security token through handshaking (see column 5, lines 57-61 and column 8, lines 33-37) similar to the one described in fig. 1 (see column 1, line 55 through column 2, line 36) that meets the recitation of *receiving a first security token from the first program*;

the handshaking session used (i.e. key or password) meets the recitation of security token associating with the first connection (*associating the first security token with the first connection)* (see column 7, lines 40-64 and column 8, lines 33-37 and column 9, lines 3-5);

creating a second connection between relay and server (see column 8, lines 17-19 and column 10, lines 61-62) that meets the recitation *of creating a second connection to a relay program*;

providing the first security token to the relay program, for example (see column 5, lines 10-13 and column 9, lines 3-5); *and upon successful creation of the second connection, coupling the first connection to the second connection*, for example(see column 8, lines 50-65).

Aziz et al does not explicitly disclose creating a first connection to a first program. **Crichton et al** in an analogous art teaches using a client proxy for communicating with a client and with a middle proxy and coupling the connections to provide end-to-end connections through firewalls (column 2, lines 26-52). **Crichton et al** also discloses the client and the proxy can reside on the same machine (column 6, lines 15-24). **Crichton et al** also discloses that the functionality of end proxies that meets the recitation of protocol daemon can be increased to allow for other protocols and services, for example one end proxy could provide both client and server end proxy functionality (column 5, lines 41-45). **Crichton et al** discloses one end proxy could provide both client and server end proxy functionality (column 5, lines 41-45). This means if the first program represents an application server an in-bound connection is created "a server end-proxy can connect to an inside X-Windows system server and a middle proxy" (column 5, lines 32-35). Applicant's specification discloses the same (on page 9, lines 9-15) program 135 (first program) requires an in-bound connection (e.g. where program 135 is an application server) … such functionality is provided by a daemon running on computer 105. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify **Aziz et al** to provide a protocol daemon program that does the creating of the first connection to a first program as well as the second connection and coupling the first and second connections thus increasing the functionality of end proxy to allow for other protocols and services as suggested by **Crichton et al (**see column 5, lines 32-45). One skilled in the art would have been lead to make such a modification and recognizes the advantage of using an end proxy that could provide both client and server end proxy functionality as this increase of functionality would allow for more protocols and services as suggested by **Crichton et al** (see column 5, lines 41-45).

As per claim 121, the references as combined above disclose the limitation of wherein the second connection is transmitted through a firewall program (see **Crichton et al**, fig. 4). Claim 121 is rejected on the same rationale as the rejection of claim 120.

As per claim 122, the references as combined above disclose relaying a data stream between the first connection and the second connection (see **Aziz et al,** column 8, lines 50-65).

As per claim 123, the references as combined above disclose wherein the first security token is one of a password and a verification string (see **Aziz et al,** column 9, lines 3-5).

As per claim 124, the references as combined above disclose terminating the first connection and the second connection (see **Aziz et al,** column 8, lines 48-49).

As per claims 128-130, Aziz et al discloses *receiving a first security token from the first program* (see column 5, lines 57-61 and column 8, lines 33-37; *providing the first security token to the relay program*, for example (see column 5, lines 10-13 and column 9, lines 3-5) a relay program for relaying first connection with second connection (see abstract and column 9, lines 30-39 and column 8, lines 50-65), and further discloses either the client, the server, or the relay may be a protocol daemon and may be incorporated in one or more machines (see column 6, lines 4-6). **Aziz et al** does not explicitly disclose a protocol daemon does the creating the first connection, the creating the second connection. **Crichton et al** in an analogous art teaches using a client proxy for communicating with a client and with a middle proxy and coupling the connections to provide end-to-end connections through firewalls (column 2, lines 26-52). **Crichton et al** also discloses the client and the proxy can reside on the same machine (column 6, lines 15-24). **Crichton et al** also discloses that the functionality of end proxies that meets the recitation of protocol daemon can be increased to allow for other protocols and services, for example one end proxy could provide both client and server end proxy functionality (column 5, lines 41-45). **Crichton et al** discloses the protocol daemon creating connection as explained in claim 12 above. Claims 128-130 are rejected on the same rationale as the rejection of claim 120 above.

As per claim 140, Aziz et al discloses an apparatus comprising: a relay (220 and 440, figures 2 and 4) having means for receiving from a client or first computer (first program) a first security token through handshaking (see column 5, lines 57-61 and column 8, lines 33-37) similar to the one described in fig. 1 (see column 1, line 55 through column 2, line 36) that meets the recitation of *means for receiving a first security token from the first program* (column 5, lines 18-20);

the handshaking session used (i.e. key or password) meets the recitation of security token associating with the first connection (*means for associating the first security token with the first connection)* (see column 7, lines 40-64 and column 8, lines 33-37 and column 9, lines 3-5);

the relay (220 and 440, figures 2 and 4) having means for creating a second connection between relay and server (see column 8, lines 17-19 and column 10, lines 61-62) that meets the recitation *of means for creating a second connection to a relay program*;

means for providing the first security token to the relay program, for example (see column 5, lines 10-13 and column 9, lines 3-5); *and upon successful creation of the second connection, means for coupling the first connection to the second connection*, for example(see column 8, lines 50-65).

Aziz et al does disclose that the relay may be used as a daemon (column 6, lines 4-6) but is silent about means for creating a first connection to a first program, **Crichton et al** in an analogous art teaches using a client proxy for communicating with a client and with a middle proxy and coupling the connections to provide end-to-end connections through firewalls (column 2, lines 26-52). **Crichton et al** also discloses the client and the proxy can reside on the same machine (column 6, lines 15-24). **Crichton et al** also discloses that the functionality of end proxies that meets the recitation of protocol daemon can be increased to allow for other protocols and services, for example one end proxy could provide both client and server end proxy functionality (column 5, lines 41-45). **Crichton et al** discloses one end proxy could provide both client and server end proxy functionality (column 5, lines 41-45). This means if the first program represents an application server an in-bound connection is created "a server end-proxy can connect to an inside X-Windows system server and a middle proxy" (column 5, lines 32-35). Applicant's specification discloses the same (on page 9, lines 9-15) program 135 (first program) requires an in-bound connection (e.g. where program 135 is an application server) ... such functionality is provided by a daemon running on computer 105. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify **Aziz et al** to provide a protocol daemon program that does the creating of the first connection to a first program as well as the second connection and coupling the first and second connections thus increasing the functionality of end proxy to allow for other protocols and services as suggested by **Crichton et al (**see column 5, lines 32-45). One skilled in the art would have been lead to make such a modification and recognizes the advantage of using an end proxy that could provide both client and server end proxy functionality as this increase of functionality would allow for more protocols and services as suggested by **Crichton et al** (see column 5, lines 41-45).

As per claim 141, the references as combined above disclose means for transmitting the second connection through a firewall program (see **Crichton et al**, fig. 4). Claim 141 is rejected on the same rationale as the rejection of claim 140.

As per claim 142, the references as combined above disclose a relay having means for relaying a data stream between the first connection and the second connection (see **Aziz et al,** column 8, lines 50-65).

As per claim 143, the references as combined above disclose wherein the first security token is one of a password and a verification string (see **Aziz et al,** column 9, lines 3-5).

As per claim 144, the references as combined above disclose means for terminating the first connection and the second connection (see **Aziz et al,** column 8, lines 48-49).

Claims 174-178 contain the same limitations as claims 120-124 respectively except for incorporating the claimed method into a computer program. Therefore, 174-178 are rejected on the same rationale as the rejection of claims 120-124.

7. **Claims 125-127, 145-147, and 179-181** are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent 6,643,701 to **Aziz et al** in view of US Patent 6,104,716 to **Crichton et al**. as applied to claims 120-124, 140-144, and 174-178 and further in view of US Patent 6,064,671 to **Killian.**

As per claims 125-127, Crichton et al discloses that the functionality of end proxies that meets the recitation of protocol daemon can be increased to allow for other protocols and services, for example one end proxy could provide both client and server end proxy functionality (column 5, lines 41-45) that meets the recitation of claim 126. **Aziz et al** discloses a relay that compares the first security token of the client with stored tokens to perform authentication and in response to a match (i.e. the client's password matches the stored password), coupling the second connection (connection between relay and server) to the first connection which matches the stored security token (see column 12, lines 8-21; column 7, line 65 through column 8, line 1; column 2, lines 11-15). **Aziz et al** does not explicitly disclose including the second connection with one or more corresponding connections in response to no match. **Killian** in an analogous art teaches providing a plurality of sockets in a socket table or array, wherein each socket normally represents a connection (i.e. has an associated connection) and each socket has an associated network port and network IP address (see column 14, lines 52-64 and column 15, lines 60-67 and column 5, lines 15-22). **Killian** further discloses means for comparing the network address with the associated network addresses for a match in the socket table (see column 16, lines 6-12 and fig. 3) that meets the recitation of comparing the first security token with the associated security tokens; in response to said comparing if none of the associated security tokens match the first security token (see column 16, lines 17-20), including the socket in the plurality of sockets (see column 16, lines 25-28). **Killian** also suggests handshaking including use of password (see column 22, lines 3-11). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method as combined above to associate the connections with a security token and create new entry in the table in response to no match because it would allow to keep track on the traffic on the network which provides an advantage in load balancing as suggested by **Aziz et al** (see column 9, lines 31-35 and lines 42-48).

As per claims 145-147, Crichton et al discloses that the functionality of end proxies that meets the recitation of protocol daemon can be increased to allow for other protocols and services, for example one end proxy could provide both client and server end proxy functionality (column 5, lines 41-45) that meets the recitation of claim 146. **Aziz et al** discloses a relay with means for comparing the first security token of the client with stored tokens to perform authentication and in response to a match (i.e. the client's password matches the stored password), means for coupling the second connection (connection between relay and server) to the first connection which matches the stored security token (see column 12, lines 8-21; column 7, line 65 through column 8, line 1; column 2, lines 11-15). **Aziz et al** does not explicitly disclose including the second connection with one or more corresponding connections in response to no match. **Killian** in an analogous art teaches means for providing a plurality of sockets in a socket table or array, wherein each socket normally represents a connection (i.e. has an associated connection) and each socket has an associated network port and network IP address (see column 14, lines 52-64 and column 15, lines 60-67 and column 5, lines 15-22). **Killian** further discloses means for comparing the network address with the associated network addresses for a match in the socket table (see column 16, lines 6-12 and fig. 3) that meets the recitation of means for comparing the first security token with the associated security tokens; in response to said comparing if none of the associated security tokens match the first security token (see column 16, lines 17-20), means for including the socket in the plurality of sockets (see column 16, lines 25-28). **Killian** also suggests handshaking including use of password (see column 22, lines 3-11). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method as combined above to associate the connections with a security token and create new entry in the table in response to no match because it would allow to keep track on the traffic on the network which provides an advantage in load balancing as suggested by **Aziz et al** (see column 9, lines 31-35 and lines 42-48).

Claims 179-181 contains the same limitations as claims 125-127 respectively except for incorporating the claimed method into a computer program. Therefore, 179-181 are rejected on the same rationale as the rejection of claims 125-127.

Conclusion

8. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. (See PTO-form 892).

8.1 Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL.** See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

8.2 Any inquiry concerning this communication or earlier communications from the examiner should be directed to Carl Colin whose telephone number is 571-272-3862. The examiner can normally be reached on Monday through Thursday, 8:00-6:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser G. Moazzami can be reached on 571-272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/C.C./

Carl Colin
Patent Examiner
October 14, 2007

NASSER MOAZZAMI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

10/15/07